P24933.P04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Chil Min KIM et al.

Serial No. : Not Yet Assigned

Filed : Concurrently Herewith

For : ENCRYPTION AND COMMUNICATION APPARATUS AND METHOD USING MODULATED DELAY TIME FEEDBACK CHAOTIC SYSTEM

CLAIM OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Applicant hereby claims the right of priority granted pursuant to 35 U.S.C. 119 based upon Korean Application No. 10-2003-0074183, filed October 23, 2003. As required by 37 C.F.R. 1.55, a certified copy of the Korean application is being submitted herewith.

Respectfully submitted,
Chil Min KIM et al.

Leslie J. Depperman Reg. No. 33,329

Bruce H. Bernstein
Reg. No. 29,027

February 17, 2004
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0074183
Application Number

출 원 년 월 일 : 2003년 10월 23일
Date of Application OCT 23, 2003

출 원 인 : 학교법인 배재학당
Applicant(s) PAI CHAI UNIBERSITY

2004 년 01 월 26 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2003.10.23
【발명의 명칭】	시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치와 그 방법
【발명의 영문명칭】	APPARATUS FOR CONVERTING AND TRANSMITTING A CODE USING CHAOS SYSTEM AND THE METHOD THEREFOR
【출원인】	
【명칭】	학교법인 배재학당
【출원인코드】	2-1999-902417-2
【대리인】	
【성명】	심서래
【대리인코드】	9-1998-000294-1
【포괄위임등록번호】	1999-002963-3
【발명자】	
【성명의 국문표기】	김칠민
【성명의 영문표기】	KIM,Chil Min
【주민등록번호】	550824-1120610
【우편번호】	306-787
【주소】	대전광역시 대덕구 오정동 신동아아파트 2동 509호
【국적】	KR
【발명자】	
【성명의 국문표기】	계원호
【성명의 영문표기】	KYE,Won Ho
【주민등록번호】	660117-1051411
【우편번호】	302-782
【주소】	대전광역시 서구 삼천동 국화아파트 304동 105호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 심서래 (인)

1020030074183 출력 일자: 2004/1/27

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	15	면	15,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	14	항	557,000 원
【합계】	601,000 원		
【감면사유】	학교		
【감면후 수수료】	300,500 원		

【요약서】

【요약】

본 발명은 혼돈시스템을 이용한 암호화 장치에 있어서, 원래의 혼돈신호와 소정의 되먹임되는 혼돈신호에 따른 고차원의 혼돈신호를 발생하는 혼돈신호발생수단과; 상기 혼돈신호발생수단에서 출력하는 혼돈신호를 일정시간 지연시킨 후 시간지연혼돈신호를 변조하는 지연시간변조수단; 및 상기 혼돈신호발생수단에서 발생되는 혼돈신호와 지연시간변조수단에서 출력되는 시간지연변조신호를 각각 제공받아 가감한 후 상기 혼돈신호발생수단으로 되먹이는 되먹임수단;을 각각 구비하여, 혼돈신호 속에 내재된 정보신호를 외부에서 공격할 수 없도록 지연시간을 변조시킴으로써, 시간지연 되먹임 혼돈신호 속에서 시간지연이 변조되고 있으므로 그 속에 포함된 정확한 지연시간을 파악할 수 없음에 따라 정보신호를 해독하는 것이 불가능하여 보다 견고하고 신뢰성있는 암호화시스템을 구축할 수 있는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치와 그 방법을 제공한다.

【대표도】

도 2

【명세서】

【발명의 명칭】

시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치와 그 방법{APPARATUS FOR CONVERTING AND TRANSMITTING A CODE USING CHAOS SYSTEM AND THE METHOD THEREFOR}

【도면의 간단한 설명】

도 1은 본 발명에 의한 시간지연변조 되먹임 혼돈시스템을 이용한 암호화장치를 나타낸 블록도이고,

도 2는 본 발명의 일실시예에 의한 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치를 나타낸 회로 블록도이고,

도 3a 내지 도 3c는 본 발명에 의한 로지스틱 맵의 자체 상관관계에서 나타나는 시간지연정보를 설명하기 위한 도면이고,

도 4a 및 도 4b는 본 발명에 의한 로렌쯔 혼돈계에서 지연시간변조 되먹에 의한 혼돈 끌개의 모양을 나타낸 도면이고,

도 5a 및 도 5b는 본 발명에 의한 로렌쯔 혼돈계에서 자체 상관관계에서 나타나는 시간지연정보를 설명하기 위한 도면이고,

도 6a 및 도 6b는 본 발명에 의한 두 로렌쯔 혼돈계의 가로 리야푸노프 지수를 설명하기 위해 도시한 도면이고,

도 7은 본 발명에 의한 두 로렌쯔 혼돈계가 동기화되는 영역을 설명하기 위한 도면이고,

도 8a 내지 도 8c는 본 발명에 의한 두 로렌쯔 혼돈계가 동기화되는 모양을 설명하기 위해 도시한 도면이다.

* 도면의 주요 부분에 대한 부호의 설명

1: 혼돈시스템	10: 혼돈신호발생장치
20: 시간지연장치	30: 지연시간변조장치
40: 되먹임수단	100: 암호화장치
110: 제 1 혼돈신호발생장치	120: 시간지연변조장치
130: 되먹임수단	140: 암호화수단(가산기)
150: 송신장치	200: 복호화장치
210: 수신장치	220: 제 2 혼돈신호발생장치
230: 되먹임수단	240: 시간지연변조장치
250: 복호화수단(감산기)	

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<19> 본 발명은 혼돈시스템을 이용한 암호화 장치에 관한 것으로, 특히 시간지연 신호의 되먹임의 시간을 변조시킴으로써, 더 복잡한 혼돈신호를 발생시키는 혼돈시스템과 상기 혼돈시스템을 이용하여 암호화함에 따라 더욱 안전하게 데이터를 통신할 수 있는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치와 그 방법에 관한 것이다.

<20> 최근들어, 혼돈이론에 대한 연구가 활발히 이루어지고 있으며, 혼돈이론은 산업의 각 분야에 다양하게 적용되고 있다.

<21> 혼돈신호발생장치는 초기 조건에 민감하기 때문에 실제적으로 동일한 두 혼돈신호발생장치는 초기 조건이 극히 조금만 달라도 시간이 경과함에 따라 서로 크게 달라지고 완전히 관련 없는 상이한 궤적과 값들로 빠르게 변화한다. 즉, 시간이 경과함에 따라 혼돈신호발생장치들은 비주기적이고 예측할 수 없는 상태가 된다. 이상과 같은 혼돈신호발생장치의 현상은 나비효과(Butterfly Effect)라 불리는 초기에 민감하게 반응하는 특성에 기인한다.

<22> 혼돈시스템의 동기화란 혼돈현상을 제어하기 위하여 여러 상태 변수들을 갖는 적어도 두 개 이상의 서로 동일한 혼돈신호발생장치들로 이루어진 혼돈시스템에서 각 혼돈신호발생장치의 상태변수들이 서로 동일하게 된다는 것을 의미한다. 이러한 혼돈시스템의 동기화 기술은 산업상의 여러 분야에 응용될 수 있으며, 특히 비밀을 요구하는 통신에 매우 적합하게 응용될 수 있다.

<23> 그런데, 최근 혼돈의 동기화를 이용해 비밀통신에 적합하게 쓸 수 있는 혼돈시스템에 대한 많은 의문들이 제시되고 있다. 혼돈시스템이 저차원일 경우 혼돈예측법이나 되돌이 본뜨기를 이용하여 혼돈신호 속에 포함된 정보신호를 찾을 수 있는 방법들이 개발되었다.

<24> 이러한 이유로 고차원의 혼돈시스템을 새로운 대안으로 제시하였는데, 고차원의 혼돈시스템을 암호시스템으로 쓰면 고차원의 혼돈을 분석하는 데, 많은 시간이 걸리므로 효율적인 암호시스템으로 쓸 수 있다는 것이다. 그래서 쉽게 고차원의 혼돈을 만드는 방법으로 시간지연 되먹임에 의한 혼돈시스템을 제시하였다.

<25> 그러나, 이와 같은 고차원의 시간지연 혼돈시스템에도 문제점이 있는 것이 밝혀졌는데, 그것은 시간지연혼돈신호를 분석하면 지연시간의 정보를 알 수 있고, 지연시간을 알면 저차원의 혼돈계로 차원을 낮출 수 있어 혼돈신호 속에 내재된 정보신호를 외부에서 공격 및 유출 가능하다는 문제점이 있는 것이다.

【발명이 이루고자 하는 기술적 과제】

<26> 따라서, 본 발명의 목적은 혼돈신호 속에 내재된 정보신호를 외부에서 공격할 수 없도록 지연시간을 변조시킴으로써, 시간지연 되먹임 혼돈신호 속에서 시간지연이 변조되고 있으므로 그 속에 포함된 정확한 지연시간을 파악할 수 없어 견고한 암호화시스템을 구축할 수 있는 시간지연변조 되먹임 혼돈시스템을 이용한 암호호화 및 통신 장치와 그 방법을 제공하는 데 있다.

<27> 또한, 시간지연 되먹임 혼돈신호 속에서 시간지연이 변조되고 있으므로 그 속에 포함된 정확한 지연시간을 파악할 수 없어 혼돈시스템을 저차원으로 낮출 수 없음에 따라 보다 견고한 암호화시스템을 구축할 수 있는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치와 그 방법을 제공하는 데 있다.

【발명의 구성 및 작용】

<28> 상기 목적을 달성하기 위한 본 발명의 기술적 수단은, 혼돈시스템을 이용한 암호화 장치에 있어서: 원래의 혼돈신호와 소정의 되먹임되는 혼돈신호에 따른 고차원의 혼돈신호를 발생하는 혼돈신호발생수단; 상기 혼돈신호발생수단에서 출력하는 혼돈신호를 일정시간 지연시켜 출력하는 시간지연수단; 상기 시간지연수단에서 출력되는 시간지연혼돈신호를 변조하는 지연시간변조수단; 및 상기 혼돈신호발생수단에서 발생되는 혼돈신호와 지연시간변조수단에서 출력되는 시간지연변조신호를 각각 제공받아 가감한 후 상기 혼돈신호발생수단으로 되먹이는 되먹임수단;을 구비한 것을 특징으로 한다.

<29> 또한, 상기 목적을 달성하기 위한 본 발명의 다른 기술적 수단은, 혼돈신호를 이용하여 통신하는 혼돈시스템에 있어서: 소정의 되먹이는 혼돈신호에 따라 고차원의 혼돈신호를 발생하

는 제 1 혼돈신호발생수단, 상기 제 1 혼돈신호발생수단에서 출력되는 혼돈신호를 일정시간 지연시킨 후 변조시키는 시간지연변조수단, 상기 제 1 혼돈신호발생수단에서 발생되는 혼돈신호와 지연시간변조수단에서 출력되는 시간지연변조신호를 각각 제공받아 가감한 후 제 1 혼돈신호발생수단으로 되먹이는 되먹임수단, 상기 시간지연변조수단으로 출력되는 고차원의 암호화신호와 외부로부터 입력되는 정보신호를 가산하여 암호화하는 암호화수단, 및 상기 암호화수단을 통해 출력되는 신호를 무선 또는 유선신호 전송하는 송신수단을 구비한 암호화장치(100); 및 상기 암호화장치의 송신수단으로부터 암호화신호를 제공받는 수신수단, 소정의 되먹이는 혼돈신호에 따라 고차원의 혼돈신호를 발생하는 제 2 혼돈신호발생수단, 상기 수신수단에서 출력되는 암호화신호와 제 2 혼돈신호발생수단에서 발생되는 혼돈신호를 제공받아 가감한 후 제 2 혼돈신호발생수단으로 되먹이는 되먹임수단, 상기 제 2 혼돈신호발생수단에서 발생하는 혼돈신호를 제공받아 지연시간을 변조시키는 시간지연변조수단, 및 상기 시간지연변조수단에서 출력되는 시간지연 신호와 수신수단으로부터 입력되는 암호화신호를 감산하여 복호화하는 복호화수단을 구비한 복호화장치(200);로 이루어진 것을 특징으로 한다.

<30> 또한, 상기 목적을 달성하기 위한 본 발명의 기술적 방법은, 혼돈시스템을 이용한 암호화 및 통신 방법에 있어서: 변수들이 함수적으로 연결되어 있는 지연시간을 변조시킨 혼돈시스템으로부터 혼돈신호를 발생하는 단계; 외부로부터 입력되는 정보신호를 상기 시간지연을 변조시킨 혼돈신호에 더하여 상기 정보신호를 암호화시키는 단계; 상기 암호화된 암호신호를 전송하는 단계; 상기 전송된 암호신호를 수신받아 소정의 혼돈시스템으로 되먹이는 단계; 상기 혼돈시스템으로 출력되는 혼돈신호를 제공받아 지연시간을 변조시키는 단계; 및 상기 시간지연 변조된 혼돈신호와 수신된 암호신호를 서로 비교하여 정보신호를 추출하여 복호화하는 단계;를 수행하는 것을 특징으로 한다.

<31> 이하, 첨부한 도면을 참조하여 본 발명을 보다 상세하게 살펴보고자 한다.

<32> 도 1은 본 발명에 의한 시간지연변조 되먹임 혼돈시스템을 이용한 암호화장치를 나타낸 블록도로서, 혼돈신호발생장치(10), 시간지연장치(20), 지연시간변조장치(30) 및 되먹임장치(40)로 이루어져 있다.

<33> 상기 혼돈신호발생장치(10)는 원래의 혼돈신호와 소정의 되먹임신호에 따른 고차원의 혼돈신호를 발생하도록 구성되어 있고, 시간지연장치(20)는 혼돈신호발생장치(10)로부터 출력되는 혼돈신호를 일정시간 지연 출력하도록 구성되어 있고, 지연시간변조장치(30)는 시간지연장치(20)에서 출력되는 시간지연혼돈신호를 변조하도록 구성되어 있고, 되먹임장치(40)는 혼돈신호발생장치(10)에서 발생되는 혼돈신호와 지연시간변조장치(30)에서 출력되는 시간지연변조신호를 각각 제공받아 가감한 후 상기 혼돈신호발생장치(10)로 되먹이도록 구성되어 있다.

<34> 아울러, 상기 되먹임장치(40)는, 상기 혼돈신호발생장치(10)에서 출력되는 원래의 혼돈신호와 지연시간변조장치(30)에서 출력되는 시간지연혼돈신호를 각각 제공받아 그 차를 구하는 감산기(41)와, 상기 감산기(41)를 통해 출력되는 신호의 크기를 동기화 조건에 맞도록 크기를 조절하는 스케일링장치(43), 및 상기 스케일링장치(43)에서 출력되는 신호와 혼돈신호발생장치(10)에서 출력되는 원래의 혼돈신호를 가산하여 소정의 혼돈신호를 만든 후 혼돈신호발생장치(10)로 되먹이는 가산기(45)로 이루어져 있다.

<35> 즉, 본 발명에 따른 혼돈 시스템(1)은, 변수들이 함수적으로 연결되어 있으며 혼돈신호를 발생하는 혼돈신호발생장치(10)에서 발생하는 여러 혼돈신호 중 임의의 한 신호($x(t)$)를 시간지연장치(20)를 통해 일정시간(τ)을 지연시키면 소정의 지연신호($x(t-\tau)$)를 발생하는 데, 상기 시간지연장치(20)의 혼돈지연시간은 지연시간변조장치(30)를 통하여 지연시간을 소정의 함수($\tau = f(t)$)로 변조시키며, 상기 시간지연변조장치(30)에 의해 지연시간이 변조된 혼돈신호

는 원래의 혼돈신호와 지연신간을 변조시킨 시간지연혼돈신호의 차를 구하는 감산기(41)를 통하여 두 신호의 차이($x(t-\tau) - x(t)$)를 구하고, 그 후 스케일링장치(43)를 통하여 감산기(41)를 통과한 신호의 크기를 동기화 조건에 맞도록 크기가 $\varepsilon[x(t-\tau) - x(t)]$가 되도록 변수($\varepsilon$)를 조절한 다음, 다시 가산기(45)를 통하여 원래의 신호($x(t)$)와 스케일링장치(43)를 통과한 신호($\varepsilon[x(t-\tau) - x(t)]$)를 더하여 $x(t) + \varepsilon[x(t-\tau) - x(t)]$의 신호를 만든 다음 이 신호를 혼돈신호발생장치(10)로 되먹인다.

<36> 도 2는 본 발명의 일실시예에 의한 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치를 나타낸 회로 블록도로서, 암호화장치(100)와 복호화장치(200)를 도시한 것이다.

<37> 상기 암호화장치(100)는, 소정의 되먹이는 혼돈신호에 따라 고차원의 혼돈신호를 발생하는 제 1 혼돈신호발생장치(110)와, 상기 제 1 혼돈신호발생장치(110)에서 출력되는 혼돈신호를 일정시간 지연시킨 후 변조시키는 시간지연변조장치(120)와, 상기 제 1 혼돈신호발생장치(110)에서 발생되는 혼돈신호와 시간지연변조장치(120)에서 출력되는 시간지연변조신호를 각각 제공받아 가감한 후 제 1 혼돈신호발생장치(110)로 되먹이는 되먹임장치(130)와, 상기 시간지연변조장치(120)로 출력되는 고차원의 암호화신호와 외부로부터 입력되는 정보신호를 각각 제공받아 가산하여 암호화하는 암호화수단(100), 및 상기 암호화수단(135)을 통해 출력되는 신호를 무선 또는 유선신호를 전송하는 송신장치(150)로 구성되어 있다.

<38> 상기 암호화장치(100)의 되먹임장치(130)는, 상기 제 1 혼돈신호발생장치(110)에서 출력되는 원래의 혼돈신호와 시간지연변조장치(120)에서 출력되는 시간지연혼돈신호를 각각 제공받아 그 차를 구하는 감산기(131)와, 상기 감산기(131)를 통해 출력되는 신호의 크기를 동기화 조건에 맞도록 크기를 조절하는 스케일링장치(133), 및 상기 스케일링장치(133)에서 출력되는

신호와 제 1 혼돈신호발생장치(110)에서 출력되는 원래의 혼돈신호를 가산하여 소정의 혼돈신호를 만든 후 제 1 혼돈신호발생장치(110)로 되먹이는 가산기(135)로 이루어져 있다.

<39> 그리고, 복호화장치(200)는, 상기 암호화장치(100)의 송신장치(150)로부터 암호화신호를 제공받는 수신장치(210)와, 소정의 되먹이는 혼돈신호에 따라 고차원의 혼돈신호를 발생하는 제 2 혼돈신호발생장치(220)와, 상기 수신장치(210)에서 출력되는 암호화신호와 제 2 혼돈신호발생장치(220)에서 발생되는 혼돈신호를 제공받아 가감한 후 제 2 혼돈신호발생장치(220)로 되먹이는 되먹임장치(230)와, 상기 제 2 혼돈신호발생장치(220)에서 발생하는 혼돈신호를 제공받아 지연시간을 변조시키는 시간지연변조장치(240), 및 상기 시간지연변조장치(240)에서 출력되는 시간지연 신호와 수신장치(210)로부터 입력되는 암호화신호를 각각 제공받아 감산하여 복호화하는 복호화수단(250)으로 구성되어 있다.

<40> 아울러, 상기 복호화장치(200)의 되먹임장치(230)는, 상기 제 2 혼돈신호발생장치(220)에서 출력되는 원래의 혼돈신호와 수신장치(210)에서 출력되는 암호화신호를 각각 제공받아 그 차를 구하는 감산기(231)와, 상기 감산기(231)를 통해 출력되는 신호의 크기를 동기화 조건에 맞도록 크기를 조절하는 스케일링장치(233), 및 상기 스케일링장치(233)에서 출력되는 신호와 제 2 혼돈신호발생장치(220)에서 출력되는 원래의 혼돈신호를 가산하여 소정의 혼돈신호를 만든 후 제 2 혼돈신호발생장치(220)로 되먹이는 가산기(235)로 이루어져 있다.

<41> 즉, 상기 혼돈 시스템은 동일한 제 1 혼돈신호발생장치(110) 및 제 2 혼돈신호발생장치(220)를 구비하고 있다. 상기 제 1 혼돈신호발생장치(110)를 구비한 암호화장치(100)는 정보신호를 암호화시키는 장치이고, 상기 제 2 혼돈신호발생장치(220)를 구비한 복호화장치(200)는 암호화된 정보신호를 복호화시키는 장치이다.

<42> 상기 암호화장치(100)에서 시간지연변조장치(120)에 의해서 상기 혼돈시스템의 한 변수의 신호를 시간지연을 변조시켜 제 1 혼돈신호발생장치(110)에 되먹임으로서, 고차원의 혼돈신호를 만들어 내는데, 그 과정은 상기 도 1의 방법처럼 신호 x(t)를 시간지연을 변조시킨 혼돈신호 $x(t-\tau)$를 감산기(131)를 통하여 원래 신호와의 차이를 구하고, 이것을 스케일링장치(133)를 통하여 스케일링한 후 가산기(135)를 통하여 다시 원래 신호와 더한 후 제 1 혼돈신호발생장치(110)에 되먹여 복잡한 혼돈신호를 만들어 낸다.

<43> 이어, 암호화는 시간지연변조장치(120)를 통과한 시간지연을 변조시킨 혼돈신호에 정보신호를 가산기 또는 감산기 등의 암호화수단(140)을 거쳐서 암호신호를 만든 다음 송신장치(150)를 통하여 전송한다.

<44> 그리고, 복호화장치(200)는 암호화장치(100)로부터 전송된 암호화신호를 복호화하기 위하여 수신장치(210)를 통해 수신한 암호화신호를, 상기 제 1 혼돈신호발생장치(110)와 동일한 방법으로 제 2 혼돈신호발생장치(220)에 되먹여 상기 제 2 혼돈신호발생장치(220)를 상기 제 1 혼돈신호발생장치(110)에 동기화시키는데, 수신장치(210)에 수신된 신호와 제 2 혼돈신호발생장치(220)에서 발생하는 혼돈신호 x'(t)와의 차이를 감산기(231)를 통하여 $x(t-\tau) - x'(t)$의 신호를 구한 후 이것을 스케일링장치(233)를 거쳐 동기화 조건에 맞도록 크기가 $\varepsilon[x(t-\tau) - x(t)]$가 되도록 조절한 다음, 제 2 혼돈신호발생장치(220)의 원래 신호와 합을 가산기(235)를 통하여 $x'(t) + \varepsilon[x(t-\tau) - x'(t)]$의 신호를 만든 다음 제 2 혼돈신호발생장치(220)에 되먹인다.

<45> 그리고, 복호화는 제 2 혼돈신호발생장치(220)에서 발생하는 혼돈신호를 상기 암호화장치(100)의 시간지연변조장치(120)와 동일하게 시간지연을 변조시키는 시간지연변조장치(240)를 통과한 지연시간변조 혼돈신호와 상기 수신장치(210)를 통해 수신된 암호화신호와의 차이를

구하는 감산기와 같은 복호화수단(250)을 거치면 정보신호를 복호한 복호정보신호를 구할 수 있다.

<46> 도 3은 본 발명에 의한 로지스틱 맵(Logistic Map)을 이용하여 지연시간을 고정시켰을 때와 지연시간을 변조시켰을 때 나타나는 자체 상관관계(Auto Correlation)를 비교한 예시도이다.

<47> 이 결과에 따르면 도 3a와 같이 지연시간(τ)을 $\tau_0 = 30$으로 고정시키면, 지연시간의 정보가 ⓘ, ⓙ 및 ⓚ부분에서와 같이 나타난다. 이 지연정보가 있으면, 지연시간으로 고차원의 혼돈시스템을 만들었다 하더라도 이 고차원의 결과를 저차원으로 축소시킬 수 있어 혼돈신호 속의 정보를 알 수 있게 된다.

<48> 이에 반하여 도 3b에서처럼 지연시간(τ)을 $\tau = (\tau_0/2-1)\sin(t) + \tau_0/2$로 변조시키면 지연 자체 상관함수에 섞여 사라져 지연시간에 대한 정보가 나타나지 않는다.

<49> 이와 같은 지연시간의 희석에 의하여 지연정보를 찾을 수 없으므로 비밀의 정도가 높아지게 된다.

<50> 또한, 도 3c에서와 같이 지연시간을 $\tau = (\tau_0-1)\xi(t) + 1$이고, $\xi(t)$가 난수이면 그 지연정보 자체의 현상도 없어질 뿐만 아니라 로지스틱 맵의 신호도 난수와 같이 바뀐다. 그러므로 지연시간을 변조시켜 지연시간변조 되먹임 혼돈시스템을 이용하여 암호화시키면 정보의 안정성을 확보할 수 있다.

<51> 도 4는 로렌쯔(Lorenz) 식을 이용하여 지연시간을 변조시켜 되먹일 때 나타나는 혼돈 끌개의 모습을 도시한 것이다.

<52> 이때의 지연시간은 $\tau = 0.475\tau_0\sin(\tau t) + \tau_0/2$로 변조시켰다. 또한 되먹임은 $(1-\beta)x(t) + \beta x(t-\tau)$를 로렌쯔 혼돈계 x(t)로 되먹임 시켰다.

<53> 이 도면은 $\beta = 0.93$이며, $\omega = 0.005$일 때의 끌개의 모습인 데, 도 4a의 x-y 변수의 끌개와 도 4b의 y-z 변수의 끌개는 로렌쯔 원래의 혼돈 끌개를 갖고 있지 못해 복잡한 고차원의 혼돈신호임을 보여준다.

<54> 도 5는 로렌쯔 혼돈계에서 $\beta = 0.92$이며, $\omega = 0.005$일 때 동기화되었을 때의 자체 상관관계를 나타내는 도면이다.

<55> 도 5a는 지연시간을 고정시켰을 때 지연시간의 정보가 ⓜ부분과 같이 자체 상관관계에서 그대로 나타남을 보여주는 도면이고, 도 5b는 지연시간을 변조시켰을 때 지연시간이 자체 상관관계에서 없어지는 모양을 보여준다. 이것으로 볼 때 지연기간을 변조시켜 되먹임시키면 지연시간을 외부에서 파악할 수 없어 안전한 암호시스템으로 쓸 수 있다.

<56> 도 6a 및 도 6b는 도 5의 조건에서 두 로렌쯔 혼돈계를 동기화시킬 때, 두 로렌쯔 혼돈계가 동기화되는 것을 보여주기 위하여 구한 최대 가로 리야푸노프(Lyapunov) 지수와 두 번째 가로 리야푸노프(Lyapunov) 지수이다.

<57> 이 도면은 β와 ω에 따른 리야푸노프 지수를 구한 것인데, 두 도면 모두 리야푸노프 지수가 '0'이하의 값을 갖는 동기화 영역이 있음을 보여준다.

<58> 도 7은 두 로렌쯔 혼돈계를 결합시켰을 때 나타나는 동기화 영역을 β와 ω에 따른 영역을 구하였다.

<59> 이 도면에서 완전한 동기화가 생겨 암호시스템을 만들 수 있는 영역이 존재함을 보여준다. 여기서 CS의 영역이 동기화의 영역이다.

<60> 도 8은 두 로렌쯔 혼돈계를 동기화시켰을 때 나타나는 두 혼돈신호의 차이이다.

<61> 암호화장치(100)에서의 혼돈신호를 x_1이라 두었고, 복호화장치(200)의 혼돈신호를 x_2라 두었다.

<62> 여기서 동기화되기 전의 영역인 도 7의 ⓟ지점인 $\beta = 0.87$이고, $\omega = 0.005$일 때는 도 8a와 같이 두 신호의 차가 '0'으로 수렴하지 않으나, 동기화 영역인 도 7의 ⓠ지점인 $\beta = 0.93$이고, $\omega = 0.005$일 때는 두 혼돈계가 동기화되어 도 8b와 같이 두 혼돈계의 차이가 '0'으로 수렴한다. 이때 지연시간을 변조시킨 상태가 도 8c에 도시되어 있다.

<63> 이와 같은 본 발명에 따른 시간지연변조 되먹임 혼돈신호발생장치를 이용한 암호화 시스템 및 그 방법의 이론적 배경을 간단한 로지스틱 맵(Logistic Map)을 이용하여 살펴보기로 하자.

<64> 이러한 로지스틱 맵은 수학식 1과 같이 주어진다.

<65> 【수학식 1】 $x_{n+1} = \lambda x_n(1-x_n)$

<66> 상기 수학식 1은 혼돈현상을 나타내는 잘 알려진 수식의 하나이다. 상기 수학식 1에서 혼돈은 λ의 값에 따라 결정되는 데, 예를들어 λ가 3.9인 경우에는 제 1 혼돈신호발생장치(110)가 혼돈을 보인다.

<67> 이 로지스틱 맵에서 x_{n-N} 신호를 되먹이는데, 이때 지연시간 N을 시간에 따라 변조시켜 $N = f(t)$가 되도록 한 다음 제 1 혼돈신호발생장치(110)로 되먹인다. 이때 지연시간 N이 크면, 되먹이는 신호는 혼돈신호와의 상관관계가 없어지므로 상기 되먹이는 신호가 하나의 잡음신호로 될 수 있고, 상기 잡음신호를 암호화장치(100) 및 복호화장치(200)에 되먹이면 제 1 및 제 2 혼돈신호발생장치(110, 220)는 각각 아래의 수학식 2 및 수학식 3과 같이 주어질 수 있다.

<68> 【수학식 2】 $x_{n+1} = \lambda[x_n + \alpha(x_{n-N}-x_n)](1 - [x_n + \alpha(x_{n-N}-x_n)])$

<69> 단, x_{n-N}은 되먹임 신호이며, α는 스케일링 크기임.

<70> 【수학식 3】 $x'_{n+1} = \lambda[x'_n + \alpha(x_{n-N}-x'_n)](1 - [x'_n + \alpha(x_{n-N}-x'_n)])$

<71> 단, x_{n-N}은 되먹임 신호이며, α는 스케일링 크기임.

<72> 상기 수학식 2 및 3은 되먹임 신호와 혼돈신호의 값을 연결해 주는 결합상수 α의 값을 증가시킴에 따라 처음에는 제 1 및 제 2 혼돈신호발생장치(110, 220)는 동기화되지 않으나, 일정한 값을 넘어서게 되면 두 혼돈신호발생장치(110, 220)는 처음에는 서로 다른 초기값을 가졌더라도 나중에는 동일한 수를 발생하게 되는데, 이를 혼돈의 동기화라고 한다.

<73> 상기 동일해지는 값은 두 식의 차이식을 구하면 알 수 있게 되는데, 두 식의 차이식은 아래의 수학식 4와 같다.

<74> 【수학식 4】 $y_{n+1} = \lambda(1-\alpha)[1 - 2(1-\alpha)x_n - 2\alpha x_{n-N}]y_n + (1-\alpha)^2 y^2_n$

<75> 단, $y_n = x_n - x'_n$임.

<76> 상기 수학식 4는 새로운 비선형 차분방정식의 형태이다. 그런데, 수학식 4를 보면 먼저, y_n 앞의 매개변수로서 x_n과 x_{n-N}으로 변조되는 값이 있고, y^2_n의 매개변수에는 없다.

<77> 따라서, 수학식 4의 의미는 혼돈신호발생장치(110, 220)의 변수로 매개변수가 변조되는 새로운 식이 되는 것이다. 여기서, y_n 앞에 붙어 있는 모든 값들을 매개변수로 볼 수 있으며, 이와 같이 잡음신호로 다른 비선형계를 변조시키는 방법들은 많이 알려져 있다.

<78> 그러나, 이와 같이 잡음신호로 비선형계의 매개변수를 변조시키면 그 혼돈신호발생장치는 매우 복잡한 양상을 지니게 되는데, 각 매개변수의 조건에 따라 제 1 및 제 2 혼돈신호발생

장치(110, 220)는 혼돈신호와 '0'의 값에 가까운 값 사이를 불규칙적으로 왕복하기도 하고 '0'의 값으로 수렴할 때도 있으며, 때로는 혼돈을 보이기도 한다.

<79> 혼돈과 '0'의 값에 매우 가깝게 왕복하는 것을 온/오프 간헐성이라고 하는 데, 이러한 간헐성이 생기면 그 평균 라미나(Laminar flow)의 길이가 무한히 길어져 두 변수의 차가 '0'의 값으로 수렴하는 임계조건이 생길 수 있다.

<80> 상기 임계조건이 넘어서면, 제 1 및 제 2 혼돈신호발생장치(110, 220)의 변수차이로 만든 새로운 혼돈신호발생장치는 곧바로 '0'으로 수렴한다. 따라서, 혼돈신호발생장치의 변수차이가 '0'이 되면 제 1 및 제 2 혼돈신호발생장치(110, 220)의 궤적차가 없으므로, 제 1 및 제 2 혼돈신호발생장치(110, 220)의 궤적은 서로 같아지게 되어 곧 동기화가 된다.

<81> 이런, 형태의 식에서 평균 라미나의 길이가 무한대가 되는 조건은 이론적으로 구할 수 있다. 즉, 제 1 및 제 2 혼돈신호발생장치(110, 220)가 동기화되면 암호화를 위한 혼돈시스템으로 쓸 수 있는 것이다. 일반적으로 동기화가 생기는 영역은 일정한 영역을 가지고 있어 이 영역에서 암호화를 위한 혼돈시스템으로 쓸 수 있다.

<82> 제 1 및 제 2 혼돈신호발생장치(110, 220)가 동기화되는 영역은 리아프노프 지수(Lyapunov Exponent)의 값이 음일 때 생긴다. 그래서 혼돈이 동기화되는 조건에서 이 로지스틱 맵은 암호화 시스템으로 쓸 수 있는 것이다.

<83> 이 방법에서 지연시간을 변조시키면 도 3b와 도 3c와 같이 지연시간이 자체상관관계에서 나타나지 않아 안전한 암호시스템으로 쓸 수 있다.

<84> 이런 동기화 방법을 이용한 특성을 아래의 로렌쯔 식을 이용하여 볼 수 있다. 암호화장치(100)의 로렌쯔 혼돈시스템은 아래의 수학식 5로 주어진다.

<85> 【수학식 5】 $x_1 = \sigma(y_1 - X_1)$,

<86> $y_1 = -X_1 z_1 + rX_1 - y_1$

<87> $z_1 = X_1 y_1 - bz_1$

<88> 그리고, 복호화 장치의 수식은 아래의 수학식 6과 같이 주어진다.

<89> 【수학식 6】 $x_2 = \sigma(y_2 - X_2)$,

<90> $y_2 = -X_2 z_2 + rX_2 - y_2$

<91> $z_2 = X_2 y_2 - bz_2$

<92> 상기 수학식 5와 수학식 6에서 σ, r, b는 계수들로 각각 10.0, 28.0, 8/3으로 주었다. 그리고 암호화장치(100)의 되먹임 변수 $X_1 = (1-\beta)x_1(t) + \beta x_1(t-\tau)$로 주었으며, 복호화장치(200)의 되먹임 변수는 $X_2 = (1-\beta)x_2(t) + \beta x_1(t-\tau)$로 두어 $x_1(t-\tau)$를 두 혼돈계의 변수에 공통으로 되먹임시킨다.

<93> 이때, 지연시간은 $\tau = 0.475\tau_0 \sin(\omega t) + \tau_0/2$ 로 변조시켰다.

<94> 이런 관계에서 제 1 및 제 2 혼돈신호발생장치(110, 220)는 동기화될 수 있는데, 그것은 도 3의 로지스틱 맵에서와 같이 두 혼돈계는 동기화될 수 있다.

<95> 그럼, 제 1 및 제 2 혼돈신호발생장치(110, 220)의 로렌쯔 혼돈계가 동기화되었을 때의 지연시간을 변조시킬 때 나타나는 혼돈의 특성이 지연시간을 변조시키지 않았을 때에 비하여 어떤 장점들이 있는지를 살펴보기로 하자.

<96> 먼저, 도 4는 두 로렌쯔 식을 이용하여 지연시간을 변조시켜 되먹일 때 나타나는 혼돈끌개의 모습이다. 지연시간은 $\tau = 0.475\tau_0 \sin(\omega t) + \tau_0/2$로 변조시킬 때, $\beta = 0.93$이며, $\omega =$

0.005에서 도 4a와 도 4b에서처럼 x-y 변수의 끌개와 y-z 변수의 끌개에서처럼 로렌쯔 원래의 혼돈 끌개를 갖고 있지 못해 복잡한 고차원의 혼돈신호 임을 보여준다.

<97> 또한, 도 5는 로렌쯔 혼돈계에서 $\beta = 0.92$이며, $\omega = 0.005$일 때 동기화되었을 때의 자체 상관관계를 나타내는 도면이다.

<98> 도 5a에서처럼 지연시간을 고정시켰을 때는 지연시간의 정보가 자체 상관관계에 그대로 나타나 외부에서 정보신호의 탈취가 가능하나, 지연시간을 변조시키면 도 8b처럼 지연시간이 자체 상관관계에서 없어져 외부에서 지연시간을 외부에서 파악할 수 없어 안전한 암호시스템으로 쓸 수 있다.

<99> 이때, 도 6에 보듯이 두 로렌쯔 혼돈계가 실제로 동기화되어 암호시스템으로 쓸 수 있는지를 파악하였다. 두 로렌쯔 혼돈계를 동기화되는 조건을 구하기 위하여 최대 가로 리야푸노프(Lyapunov) 지수와 두 번째 가로 리야푸노프 지수를 도 6a와 도 6b처럼 β, ω에 따라 구하였다. 도 6a 및 도 6b 모두 리야푸노프 지수가 '0'이하의 값을 갖는 동기화 영역이 있음을 보여준다.

<100> 또한, 동기화 영역도 β와 ω에 따라 구하였는데, 도 7처럼 CS로 표시된 완전한 동기화 영역이 있어 암호시스템을 만들 수 있는 영역이 존재함을 알 수 있다.

<101> 두 로렌쯔 혼돈계를 동기화시켰을 때 나타나는 두 혼돈신호의 차이를 구하였다. 암호화장치(100)에서의 혼돈신호를 x_1이라 두었고, 복호화장치(200)의 혼돈신호를 x_2라 두었다. 여기서 동기화되기 전의 영역인 도 7의 ⓟ지점인 $\beta = 0.87$이고, $\omega = 0.005$일 때는 도 8a처럼 두 신호의 차가 '0'으로 수렴하지 않으나, 동기화 영역인 도 7의 ⓠ지점에서는 $\beta = 0.93$이고, $\omega =$

0.005일 때는 도 8b처럼 제 1 및 제 2 혼돈신호발생장치(110, 220)가 동기화되어 두 혼돈계의 차이가 '0'으로 수렴한다. 이때 지연시간을 변조시킨 상태를 도 8c에 도시하였다.

<102> 이상의 결과로 알 수 있는 것은 로지스틱 맵이나 로렌쯔 혼돈계처럼 간단한 혼돈계를 고차원 혼돈계로 만들기 위해서는 시간지연 되먹임 혼돈계로 만드는 것이 필수적이다. 그런데 이때까지 개발된 것은 지연시간을 고정시켜 되먹임으로 인하여 지연시간이 노출되어 외부에서의 공격이 용이한 문제점으로 남아 있었던 것이다.

<103> 그러나, 본 발명에서는 지연시간을 변조시키면 지연시간의 흔적이 사라지므로 외부에서 얼마의 시간만큼 지연시키는지를 알지 못하여 시간지연 되먹임 혼돈계의 고차원적 특성을 저차원으로 변환시킬 수 없으므로 안전한 암호시스템을 만들 수 있다.

<104> 아울러 이런 지연시간이 변조된 혼돈시스템을 이용하여 두 혼돈계를 동기화시킬 수 있으므로 안전한 혼돈의 동기화를 이용한 암호시스템으로 만들 수 있다.

【발명의 효과】

<105> 따라서, 본 발명에서는 혼돈신호 속에 내재된 정보신호를 외부에서 공격할 수 없도록 지연시간을 변조시킴으로써, 시간지연 되먹임 혼돈신호 속에서 시간지연이 변조되고 있으므로 그 속에 포함된 정확한 지연시간을 파악할 수 없고, 또한 정확한 지연시간을 파악할 수 없어 혼돈시스템을 저차원으로 낮출 수 없음에 따라 정보신호를 해독하는 것이 불가능하여 보다 견고하고 신뢰성있는 암호화시스템을 구축할 수 있는 이점이 있다.

【특허청구범위】

【청구항 1】

혼돈시스템을 이용한 암호화 장치에 있어서:

원래의 혼돈신호와 소정의 되먹임되는 혼돈신호에 따른 고차원의 혼돈신호를 발생하는 혼돈신호발생수단;

상기 혼돈신호발생수단에서 출력하는 혼돈신호를 일정시간 지연시킨 후 시간지연혼돈신호를 변조하는 지연시간변조수단; 및

상기 혼돈신호발생수단에서 발생되는 혼돈신호와 지연시간변조수단에서 출력되는 시간지연변조신호를 각각 제공받아 가감한 후 상기 혼돈신호발생수단으로 되먹이는 되먹임수단;을 구비한 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 장치.

【청구항 2】

청구항 1에 있어서,

상기 되먹임수단은,

상기 혼돈신호발생수단에서 출력되는 원래의 혼돈신호와 지연시간변조수단에서 출력되는 시간지연혼돈신호를 제공받아 차를 구하는 감산기;

상기 감산기를 통해 출력되는 신호의 크기를 동기화 조건에 맞도록 크기를 조절하는 스케일링수단; 및

상기 스케일링수단에서 출력되는 신호와 혼돈신호발생수단에서 출력되는 원래의 혼돈신호를 가산하여 소정의 혼돈신호를 만든 후 상기 혼돈신호발생수단으로 되먹이는 가산기;로 이루어진 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 장치.

【청구항 3】

청구항 1에 있어서,

상기 시간지연을 변조시킬 때, 변조를 주기적 신호, 준주기적 신호, 혼돈신호 또는 난수 잡음신호로 변조시키는 방식을 포함한 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 장치.

【청구항 4】

청구항 3에 있어서,

상기 시간지연을 혼돈 신호로 변조시킬 때, 혼돈 신호를 자신의 시스템의 변수를 이용하여 변조시키는 방식을 포함한 시간지연변조 시스템.

【청구항 5】

청구항 1에 있어서,

상기 시간지연변조신호를 되먹일 경우, 되먹임은 변수에 되먹이거나 계수에 되먹이거나 또는 외부 힘으로 되먹이는 방식을 사용하는 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 장치.

【청구항 6】

청구항 5에 있어서,

상기 되먹임은, 원래신호와 상기 시간지연을 변조시킨 신호를 감산기를 통하여 그 차이를 구한 후 스케일링수단을 통하여 변수 또는 계수 또는 외부 힘으로 되먹이는 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 장치.

【청구항 7】

청구항 5에 있어서,

상기 되먹임은, 상기 시간지연을 변조시킨 신호 자체를 변수, 계수 또는 외부 힘으로 직접 되먹이는 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 장치.

【청구항 8】

혼돈시스템을 이용한 암호화 및 통신 장치에 있어서:

소정의 되먹이는 혼돈신호에 따라 고차원의 혼돈신호를 발생하는 제 1 혼돈신호발생수단, 상기 제 1 혼돈신호발생수단에서 출력되는 혼돈신호를 일정시간 지연시킨 후 변조시키는 시간지연변조수단, 상기 제 1 혼돈신호발생수단에서 발생되는 혼돈신호와 지연시간변조수단에서 출력되는 시간지연변조신호를 각각 제공받아 가감한 후 제 1 혼돈신호발생수단으로 되먹이는 되먹임수단, 상기 시간지연변조수단으로 출력되는 고차원의 암호화신호와 외부로부터 입력되는 정보신호를 가산하여 암호화하는 암호화수단, 및 상기 암호화수단을 통해 출력되는 신호를 무선 또는 유선신호를 전송하는 송신수단,을 구비한 암호화장치(100); 및

상기 암호화장치의 송신수단으로부터 암호화신호를 제공받는 수신수단, 소정의 되먹이는 혼돈신호에 따라 고차원의 혼돈신호를 발생하는 제 2 혼돈신호발생수단, 상기 수신수단에서 출력되는 암호화신호와 제 2 혼돈신호발생수단에서 발생되는 혼돈신호를 제공받아 가감한 후 제 2 혼돈신호발생수단으로 되먹이는 되먹임수단, 상기 제 2 혼돈신호발생수단에서 발생하는 혼돈신호를 제공받아 지연시간을 변조시키는 시간지연변조수단, 및 상기 시간지연변조수단에서 출력되는 시간지연 신호와 수신수단으로부터 입력되는 암호화신호를 감산하여 복호화하는 복호

화수단,을 구비한 복호화장치(200);로 이루어진 것을 특징으로 하는 시간지연변조 되먹임 혼돈 시스템을 이용한 암호화 및 통신 장치.

【청구항 9】

청구항 8에 있어서,

상기 암호화장치의 되먹임수단은,

상기 제 1 혼돈신호발생수단에서 출력되는 원래의 혼돈신호와 지연시간변조수단에서 출력되는 시간지연혼돈신호를 각각 제공받아 그 차를 구하는 감산기;

상기 감산기를 통해 출력되는 신호의 크기를 동기화 조건에 맞도록 크기를 조절하는 스케일링수단; 및

상기 스케일링수단에서 출력되는 신호와 제 1 혼돈신호발생수단에서 출력되는 원래의 혼돈신호를 가산하여 소정의 혼돈신호를 만든 후 제 1 혼돈신호발생수단으로 되먹이는 가산기;로 이루어진 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치.

【청구항 10】

청구항 8에 있어서,

상기 암호화장치의 암호화수단은, 가산기인 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치.

【청구항 11】

청구항 8에 있어서,

상기 복호화장치의 되먹임수단은,

상기 제 2 혼돈신호발생수단에서 출력되는 원래의 혼돈신호와 수신수단를 통해 출력되는 암호화신호를 각각 제공받아 그 차를 구하는 감산기;

상기 감산기를 통해 출력되는 신호의 크기를 동기화 조건에 맞도록 크기를 조절하는 스케일링수단; 및

상기 스케일링수단에서 출력되는 신호와 제 2 혼돈신호발생수단에서 출력되는 원래의 혼돈신호를 가산하여 소정의 혼돈신호를 만든 후 제 2 혼돈신호발생수단으로 되먹이는 가산기;로 이루어진 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치

【청구항 12】

청구항 8에 있어서,

상기 복호화장치의 복호화수단은, 감산기인 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치.

【청구항 13】

청구항 8에 있어서,

상기 암호화된 신호를 복호화하기 위해서 제 1 혼돈신호발생수단과 제 2 혼돈신호발생수단을 동기화시키는 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 장치.

【청구항 14】

혼돈시스템을 이용한 암호화 및 통신 방법에 있어서:

변수들이 함수적으로 연결되어 있는 지연시간을 변조시킨 혼돈시스템으로부터 혼돈신호를 발생하는 단계;

외부로부터 입력되는 정보신호를 상기 시간지연을 변조시킨 혼돈신호에 더하여 상기 정보신호를 암호화시키는 단계;

상기 암호화된 암호신호를 전송하는 단계;

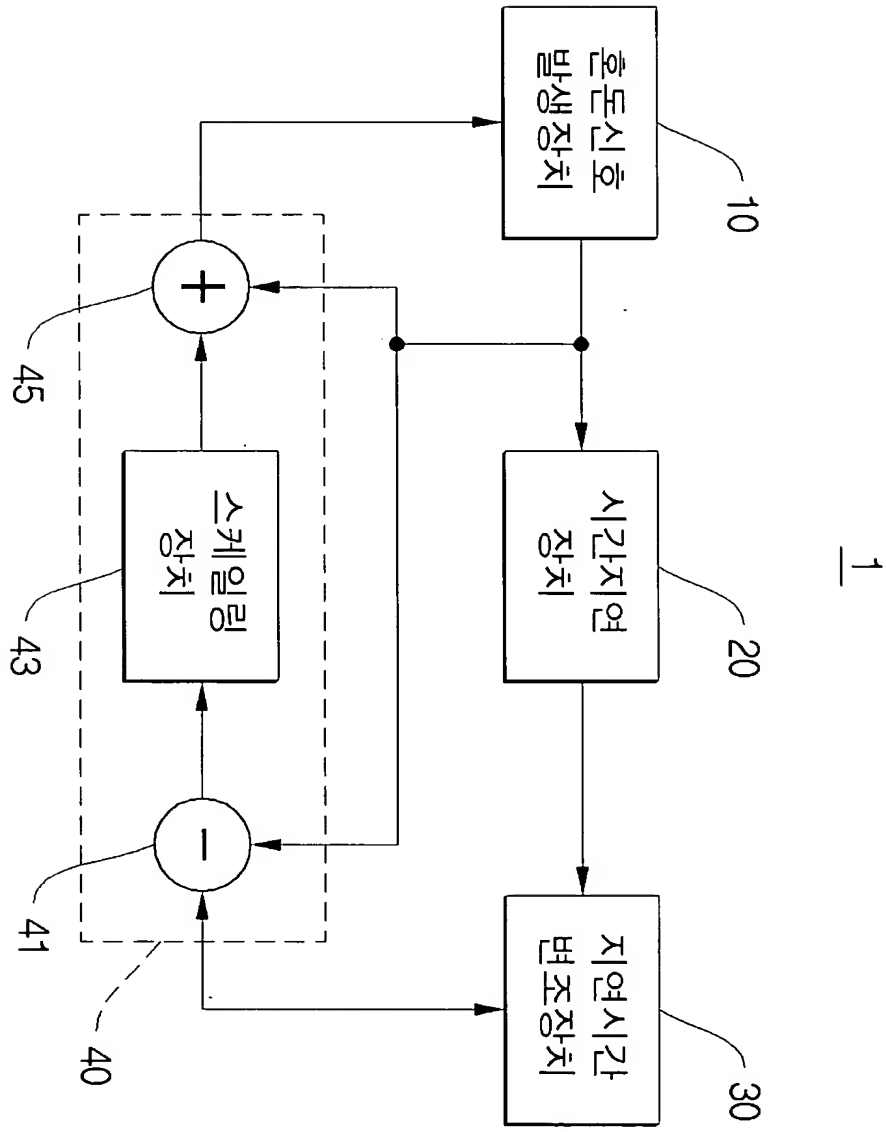
상기 전송된 암호신호를 수신받아 소정의 혼돈시스템으로 되먹이는 단계;

상기 혼돈시스템으로 출력되는 혼돈신호를 제공받아 지연시간을 변조시키는 단계; 및

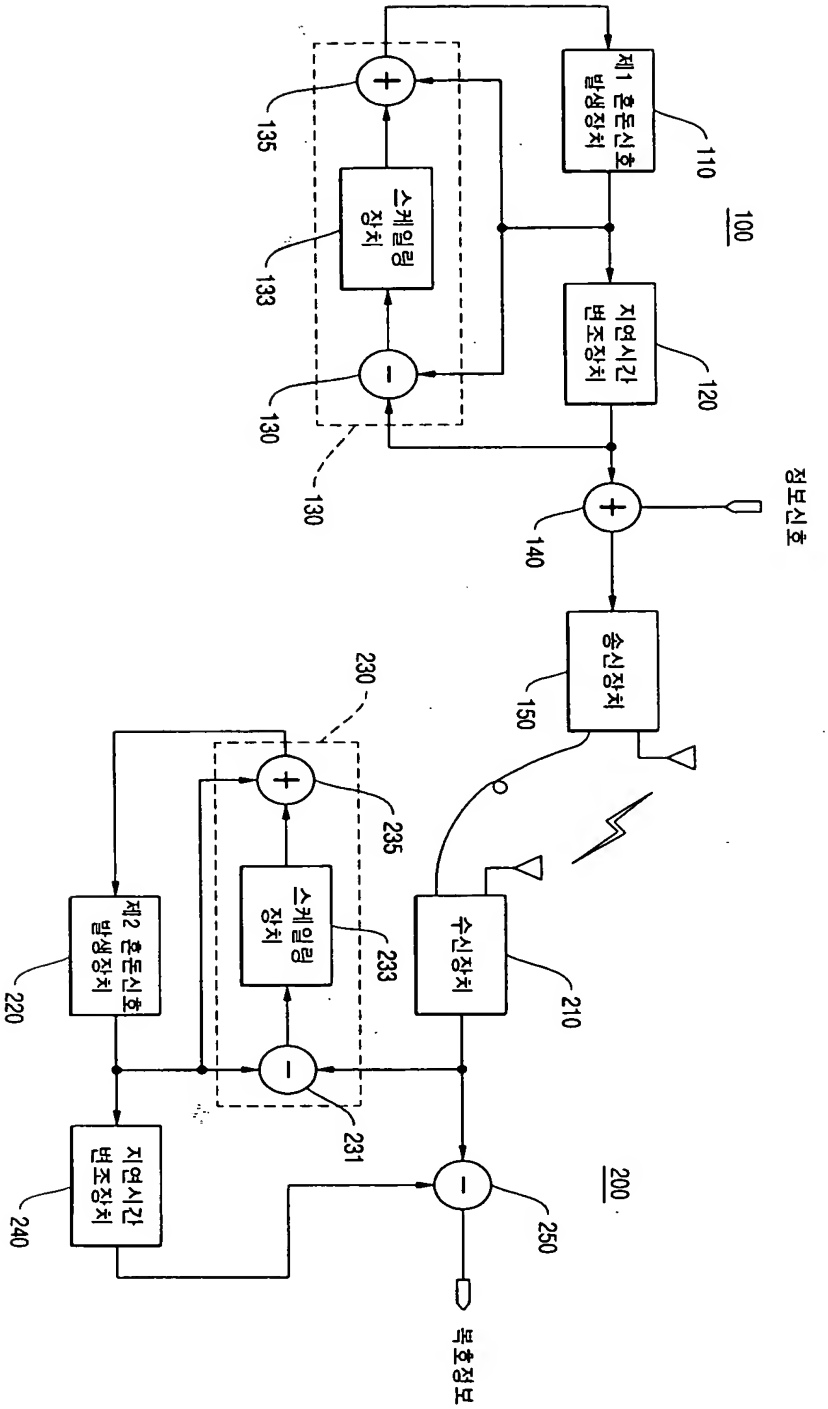
상기 시간지연 변조된 혼돈신호와 수신된 암호신호를 서로 비교하여 정보신호를 추출하여 복호화하는 단계;를 수행하는 것을 특징으로 하는 시간지연변조 되먹임 혼돈시스템을 이용한 암호화 및 통신 방법.

【도면】

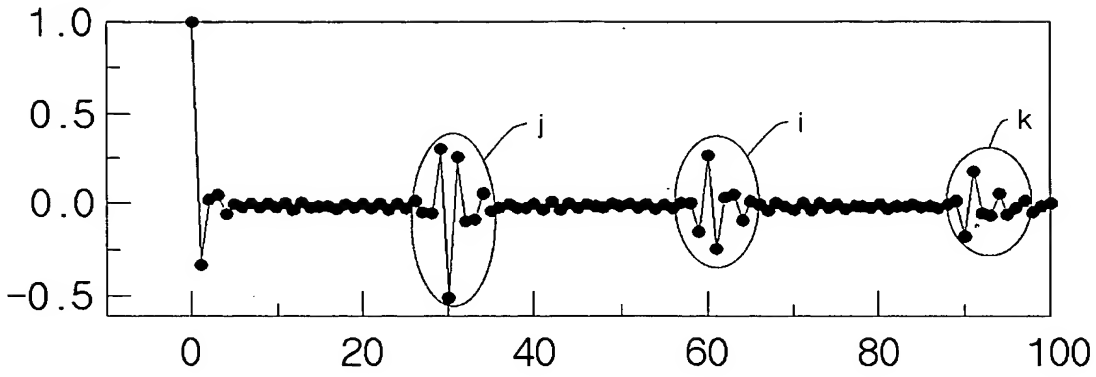
【도 1】



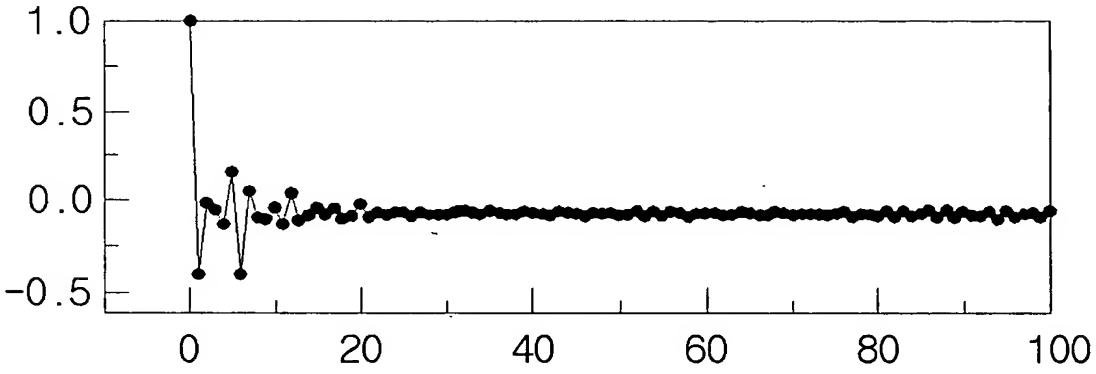
【도 2】


제1 혼돈신호 발생장치
110
100
지연시간 변조장치
120
스케일링 장치
133
135
130
130
정보신호
140
송신장치
150
230
235
스케일링 장치
233
231
제2 혼돈신호 발생장치
220
지연시간 변조장치
240
수신장치
210
200
250
복호정보

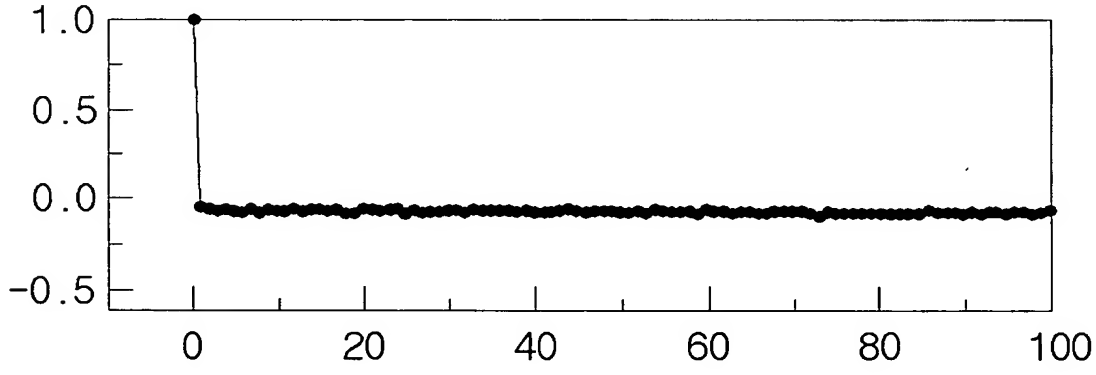
【도 3a】


1.0
0.5
0.0
-0.5
0
20
40
60
80
100
j
i
k

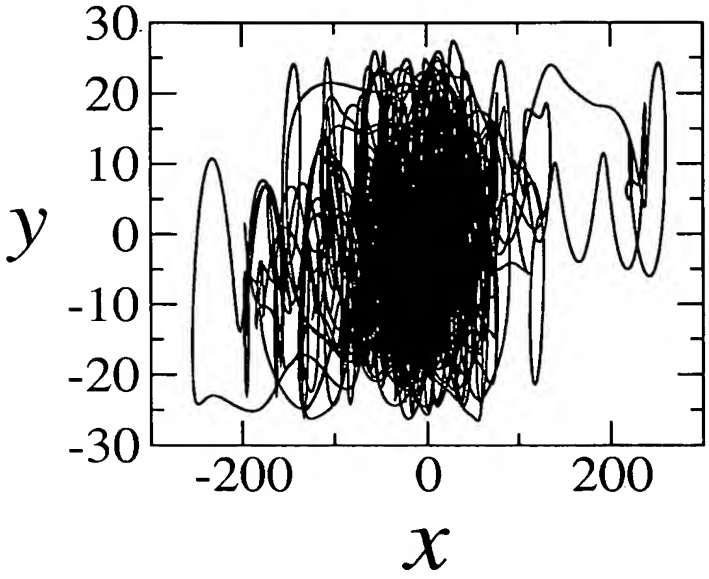
【도 3b】


1.0
0.5
0.0
-0.5
0
20
40
60
80
100

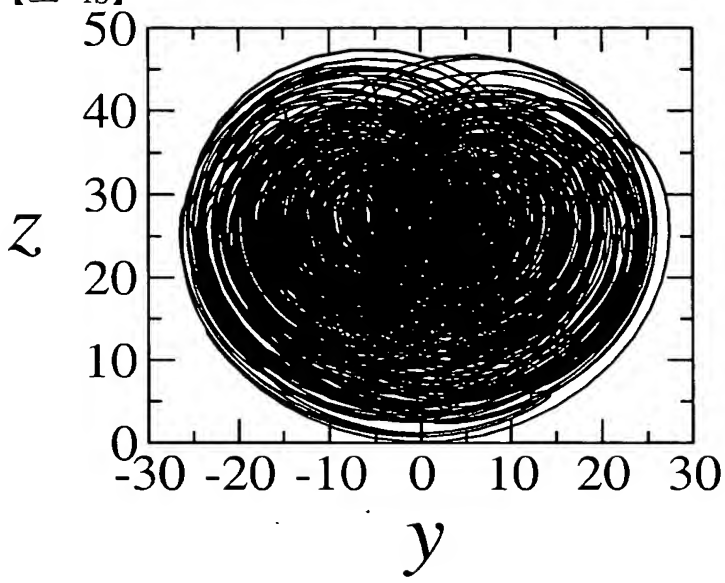
【도 3c】


1.0
0.5
0.0
-0.5
0
20
40
60
80
100

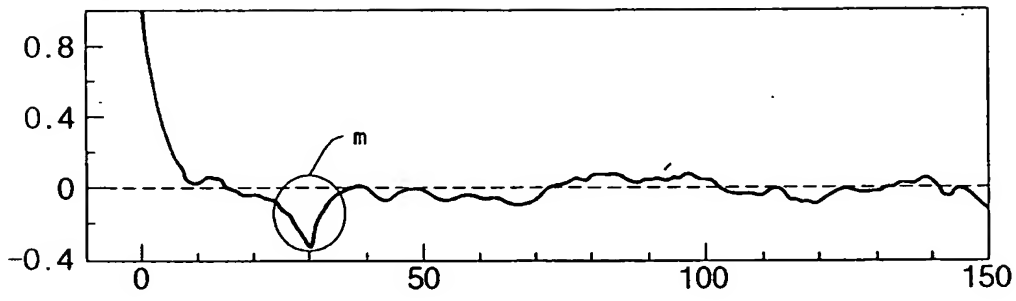
【도 4a】


30
20
10
y
0
-10
-20
-30
-200
0
200
x

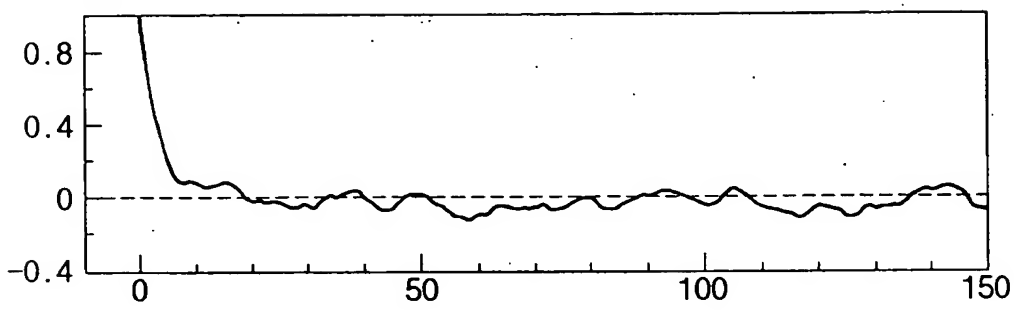
【도 4b】


50
40
30
z
20
10
0
-30 -20 -10 0 10 20 30
y

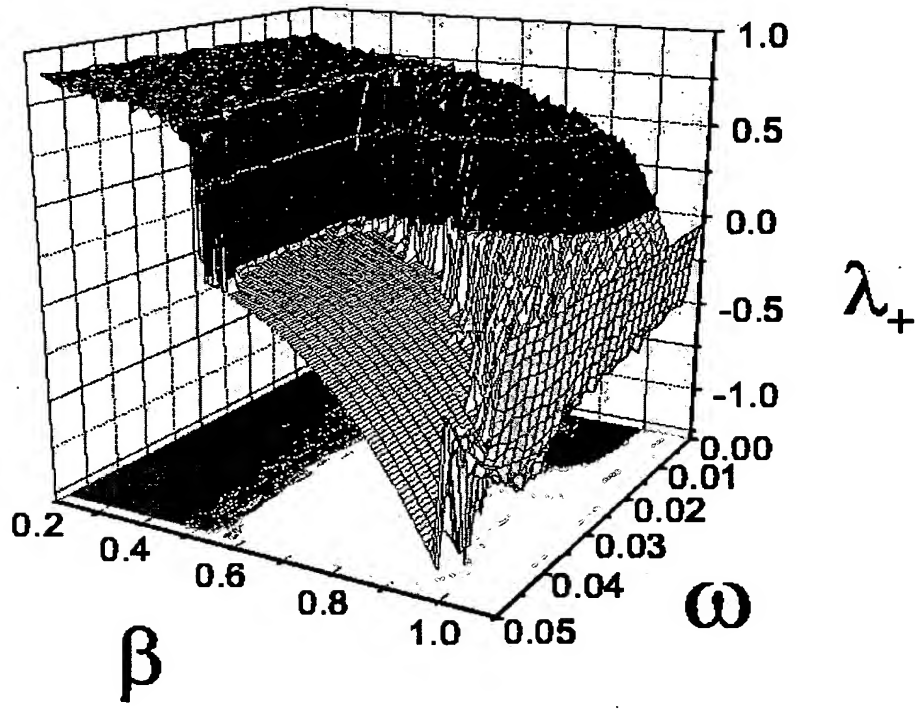
【도 5a】


0.8
0.4
0
-0.4
m
0
50
100
150

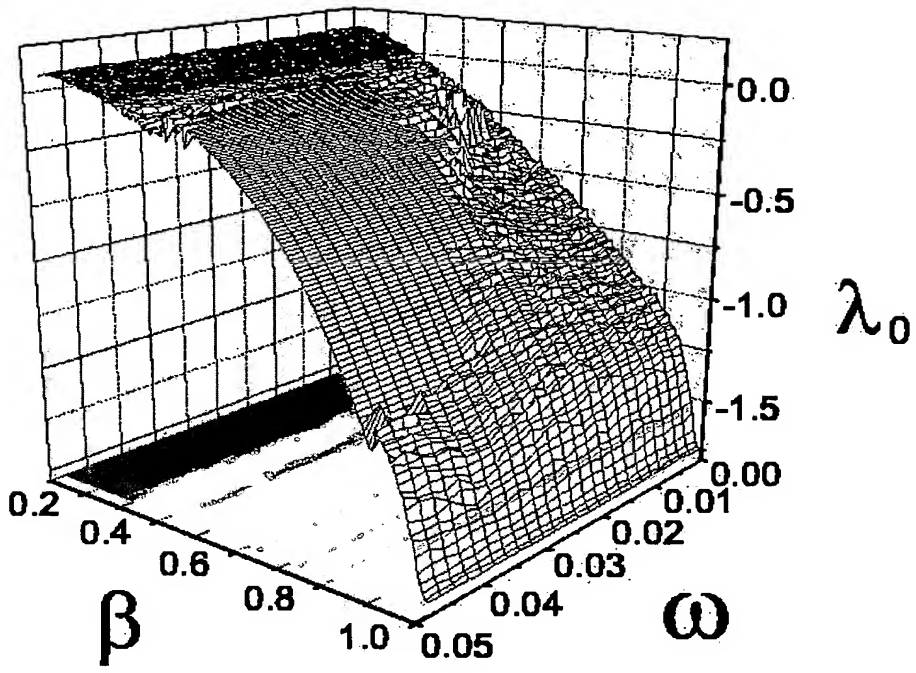
【도 5b】


0.8
0.4
0
-0.4
0
50
100
150

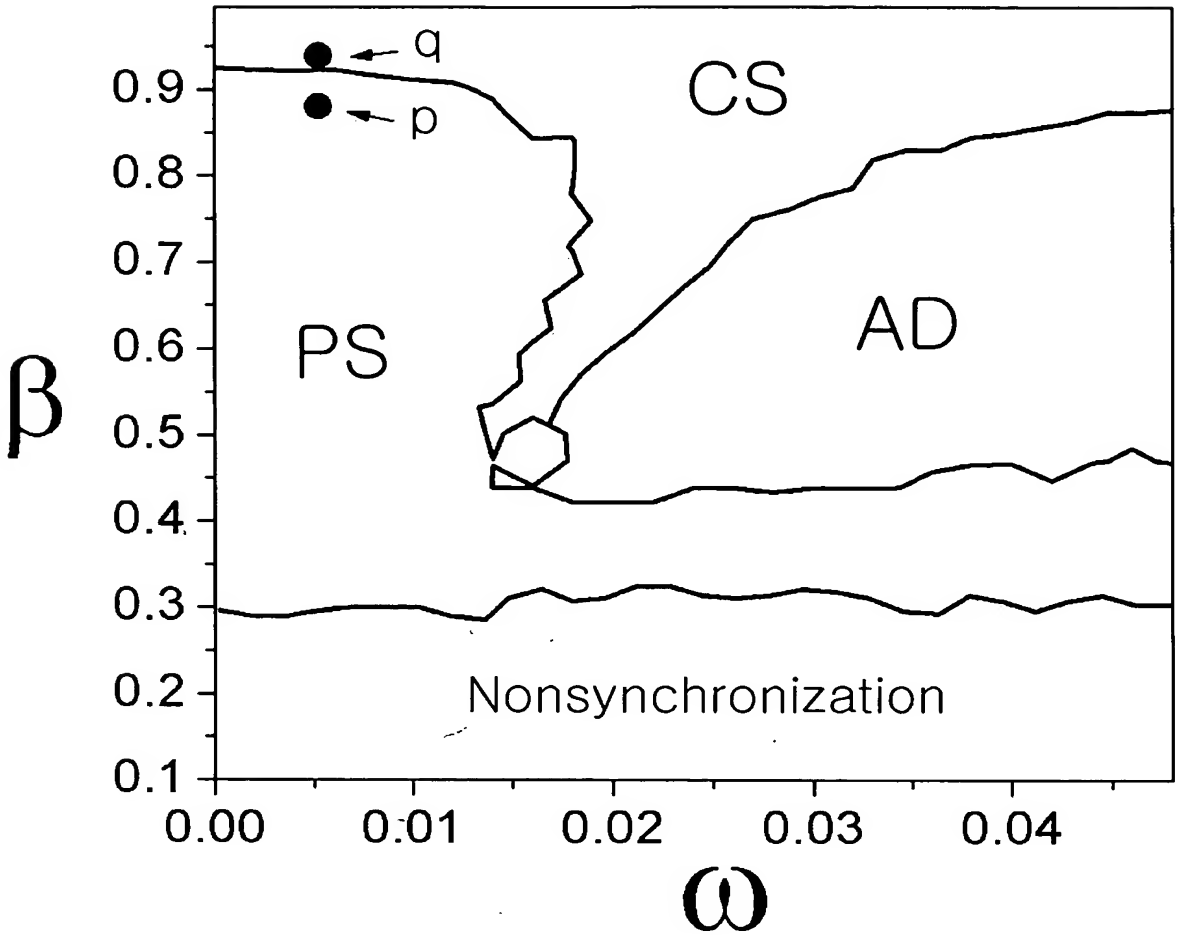
【도 6a】


1.0
0.5
0.0
-0.5
-1.0
λ_+
0.2
0.4
0.6
0.8
1.0
β
0.00
0.01
0.02
0.03
0.04
0.05
ω

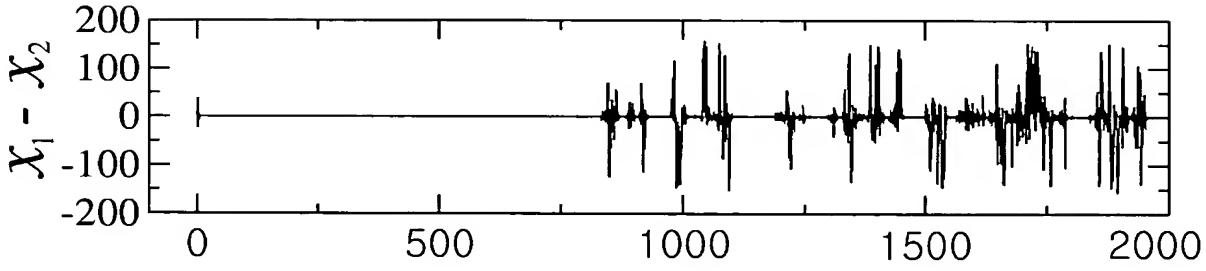
【도 6b】



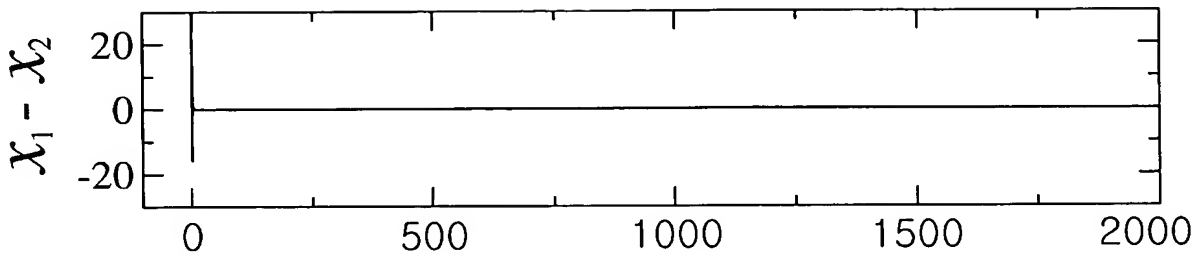
【도 7】


q
p
CS
PS
AD
Nonsynchronization
β
ω
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.00
0.01
0.02
0.03
0.04

【도 8a】


$x_1 - x_2$
200
100
0
-100
-200
0
500
1000
1500
2000

【도 8b】



【도 8c】